INTERIM STATEWIDE INFORMATION TECHNOLOGY POLICY

Interim Policy: Security of Sensitive Data

Short Title: Interim Data Security Policy

Effective Date: July 7, 2006

Approved: Richard B. Clark

Replaces and Supercedes: None

I. Policy Purpose

The purpose of this policy is to define the requirements to safeguard Sensitive Data contained on portable devices and portable electronic storage media on or off State of Montana ("State") premises, and the procedures to be followed. This policy supplements security policy ENT-SEC-112 Workstation, Portable Computer, and PDA (Personal Digital Assistant) Security.

This policy applies to all agencies and organizations that create, store or access Sensitive Data.

This policy defines the minimum requirements; agencies may adopt more stringent requirements.

Note: This Interim Policy has been developed, reviewed and implemented with an abbreviated process due to urgent business needs, and may not meet all requirements. Therefore, it will be returned for consideration and review not later than nine months from the Effective Date (VIII. Administrative Use).

II. Definitions

Refer to the Statewide Information Technology Policies and Standards Glossary for a complete list of definitions.

Sensitive Data: Refers to data that is held confidentially, and if compromised may cause harm to individual citizens or create a liability for the State. In the context of this policy, Sensitive Data is considered to be in electronic form. Examples include, but are not limited to:

1. Confidential employee information
2. Confidential citizen/individual information
3. Social Security Numbers
4. HIPAA-regulated information
5. Criminal justice information
6. Driver's license numbers

7. Trade secrets
8. Account numbers
9. Credit or debit card numbers
10. Information in combination with any required security codes, access codes, or passwords that would allow access to individual accounts.

Portable Devices: Electronic computing and communications devices designed for mobility, including laptop, desktop, and in-vehicle personal computers, personal data assistants (PDAs), cellular devices, and other devices that have the ability to store data electronically.

Portable Electronic Storage Media (Portable Storage): Includes floppy disks, CDs, DVDs, optical platters, flash memory drives, backup tapes, and other electronic storage media or devices that provide portability or mobility of data.

Secured Storage Environment: Data storage devices and support systems, such as direct attached server storage and Storage Area Network devices, managed by State personnel or provided explicitly under contract, and are secured by physical and logical means consistent with data storage best practices and Office of Cyber Protection recommendations.

Business Requirements: Requirements that can be traced back to the planning and execution of an organization's mission, goals and objectives, and its compliance to laws, regulations, policies and procedures.

III. Roles and Responsibilities

Department Heads: Under 2-15-114 MCA Security responsibilities of departments for data, each Department Head is "…is responsible for ensuring an adequate level of security for all data within that department". Specific responsibilities under this policy are:

1. Determine and define business requirements for use of Sensitive Data within their organization(s).
2. Authorize the use and storage of Sensitive Data on portable devices and portable storage within their organization(s).
3. May delegate authority to determine use of Sensitive Data on portable devices and portable storage within their organization(s).
4. Maintain an inventory and an audit trail of what Sensitive Data is used by which individuals on which portable devices and portable storage within their organization(s).
5. Enforce this policy within their organization(s).
6. Ensure that all personnel within their organization(s) are aware of this policy.

7. Inform all personnel of what constitutes Sensitive Data within their organization(s).
8. Ensure any loss, theft, or unauthorized access of Sensitive Data is reported appropriately within their organization and to the Office of Cyber Protection.

Using Personnel: Using personnel (users) are state employees, contractors, or any other individual granted access to Sensitive Data. Their responsibilities are to:

1. Determine what Sensitive Data is in their possession or accessible under their access privileges.
2. Adhere to the requirements and procedures within this policy and any special requirements or procedures issued by the Office of Cyber Protection.
3. Report as described in this policy in section IV. F. Reporting Procedures.

Office of Cyber Protection:

1. Report Sensitive Data incidents to the State CIO.
2. Maintain a library of incidents reportable under this policy to include appropriate details of each incident.
3. Define and communicate Sensitive Data report content requirements.

State CIO:

1. Determine appropriate statewide monitoring and enforcement, and actions for incidents.

IV. Requirements/ Procedures

A. Requirements

Storage of Sensitive Data is restricted:

1. Agencies shall collect, store and use Sensitive Data based on business requirements.
2. Access shall be based on business requirements and limited solely to users authorized by management.

Sensitive Data shall:

1. Not be copied or removed from Secured Storage Environments unless there is a business requirement.
2. Not be used or stored outside of State offices unless there is a business requirement approved by the department head.

3. Not be transmitted via non State-owned networks unless approved transmission protocols and encryption techniques are utilized.
4. Not be transported outside of the United States on portable devices and portable storage.
5. Only be stored on State-owned portable devices and portable storage if there is a business requirement.
6. Be encrypted when taken off State premises on portable devices and portable storage.
7. Not be transferred to non State-owned portable devices or portable storage unless there is a business requirement.

Each agency shall:

1. Document business requirements for Sensitive Data. Documentation shall be available to appropriate agency IT staff and management.
2. Maintain a documented audit trail (including a date/time record of significant changes) and inventory of:
    - who has what Sensitive Data
    - what is the business requirement
    - what portable devices or storage are used

B. Device Configuration Procedures

Users of portable devices containing Sensitive Data are required to configure and properly secure the device. Based upon device capability:

1. Configure the device as required in policy ENT-SEC-112.
2. Configure the login banner to be enabled during travel, adding contact information and explicit instructions on how to return the portable device to the information required by policy ENT-SEC-112.
3. Disable file- and print-sharing functions.
4. Ensure there is a required login for the operating system.
5. Disable Auto-Logon features.
6. Use passwords that conform to the requirements and guidelines of statewide IT security policy ENT-SEC-063 - Usernames and Passwords.
7. Ensure there is a backup of data within a Secured Storage Environment.

C. Physical Security Procedures

Physical security procedures undertaken by users with portable devices and portable storage containing Sensitive Data in their custody includes the following requirements:

1. Ensure the portable device has an asset/property tag containing appropriate contact information.
2. Label all portable device components and portable storage for individual identification.
3. Do not leave portable devices and portable storage unattended in non-secured areas.
4. Do not leave the portable device or portable storage in an unlocked vehicle; place the devices and storage in a locked trunk or out of plain sight in the locked passenger compartment.
5. Store portable devices and portable storage in a safe when staying in a hotel.
6. Monitor the whereabouts of the portable device and portable storage as they pass through airport security checkpoints and retrieve them as soon as possible to minimize the risk of loss or theft.
7. Confer with departmental technical support or the Office of Cyber Protection for specific technology selections and implementation procedures for encryption of data.

D. Operational Procedures

When accessing Sensitive Data resident on Secured Storage Environments from a non-state network with portable devices:

1. Access Sensitive Data using only secure web clients.
2. Do not transfer Sensitive Data to another device or storage not in compliance with this policy.

E. Procedures for Travel Outside of the United States

Traveling outside of the United States requires more stringent security requirements. When traveling outside of the United States with portable devices or portable storage:

1. Prior to travel remove any Sensitive Data from the portable devices and portable storage.
2. During travel do not store Sensitive Data on portable devices and portable storage.

F. Reporting Procedures

Using personnel shall report incidents involving Sensitive Data in their custody as follows:

1. Immediately report loss or theft of Sensitive Data to appropriate law enforcement agencies.
2. As soon as practical report loss, theft, or unauthorized access of Sensitive Data or security-related incidents to a supervisor and the Office of Cyber Protection.
3. Document the details of any loss, theft, unauthorized access of portable device or portable storage, or security-related incident; and deliver the document to the Office of Cyber Protection within five business days.
4. Any person aware of an unreported loss, theft or compromise of Sensitive Data shall make a report to their supervisor and the Office of Cyber Protection as soon as practical.

G. Compliance

Compliance shall be indicated by individual and organizational adherence to the requirements and procedures of this policy.

H. Enforcement

Each agency is responsible for the implementation and enforcement of this policy. The State CIO will monitor agency compliance and may take additional enforcement actions. Enforcement actions for violations of this policy include, but are not limited to:

- Disciplinary action for individuals, up to and including termination
- Denial of access to Sensitive Data
- Revocation of network access privileges

Other enforcement actions may be taken under 2-17-514(1), MCA. In addition, organizations and individuals may be liable for costs incurred as a result of loss, theft or unauthorized access of Sensitive Data.

V. Change Control and Exceptions

Policy changes or exceptions are governed by the Policy for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form.

VI. Closing

For questions or comments on this interim policy, e-mail ITpolicy@mt.gov, or, contact the Information Technology Services Division at:

Chief Information Officer
PO Box 200113

Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

The technical contact for this interim policy is:

Office of Cyber Protection (OCP)
910 Helena Avenue
Helena, Montana 59620-0116
(406) 444-4510
FAX: (406) 444-4644
doaitsd/ocp@mt.gov

VII. Cross-Reference Guide

A. State/Federal Laws

- 45 CFR Part 160 General Administrative Requirements
- 45 CFR Part 164, Subpart C Security Standards for the Protection of Electronic Protected Health Information
- 2-17-514, MCA - Department -- Enforcement Responsibilities
- 2-17-534, MCA - Security responsibilities of department
- 2-15-114, MCA - Security responsibilities of departments for data
- 45-6-311, MCA - Unlawful use of a computer

B. State Policies (IT Policies, MOM Policies, ARM Policies):

- Policy for Establishing and Implementing Statewide Information Technology Policies and Standards (pending)
  - Action Request for Statewide IT Policies or Standards
  - Exception Request for Statewide IT Policies or Standards
- ENT-063 Usernames and Passwords
- ENT-SEC-112 Workstation, Portable Computer, and PDA (Personal Digital Assistant) Security
- 1-0250.00, MOM

C. IT Procedures or Guidelines Supporting this Policy

None.

VIII. Administrative Use

History Log	
Approved Date:	July 7, 2006

Effective Date:	July 7, 2006
Change & Review Contact:	ITpolicy@mt.gov
Review:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	Nine months from Effective Date
Last Review/Revision:	
Changes:	